

Microsoft 365 Assessments: Detailed Scope & Deliverables

Compare assessment options, included reports, evidence sources, and remediation outputs.

HOW TO USE THIS GUIDE

Each assessment is designed for a different decision point. Use the comparison below to identify the best starting point, then review the detailed page for the reports, evidence, and remediation guidance included.

ASSESSMENT	WHEN TO CHOOSE IT
01 Microsoft 365 Baseline Security	A broad health check and prioritized hardening roadmap for core Microsoft 365 controls.
02 Microsoft 365 Security & Data Governance	A deeper review of collaboration exposure, data protection, retention, and governance maturity.
03 Microsoft 365 Copilot & AI Readiness	Preparation for Copilot or broader AI adoption, with focus on data access, permissions, and governance.
04 Microsoft 365 Copilot & AI Agent / Non-Human Identity	Discovery and risk review of AI agents, applications, service principals, automation, and other non-human identities.
05 Cyber Insurance Evidence Pack	Documented, classified evidence for cyber insurance applications, renewals, and underwriting follow-up.

Evidence principle

Unavailable evidence is identified as a validation requirement or collection limitation. It is not treated as proof that a control is effective.

Microsoft 365 Baseline Security

OVERVIEW

Establish a practical security baseline across identity, access, collaboration, email, endpoints, and administrative controls.

BEST FIT

Best for teams that need a broad Microsoft 365 health check, a prioritized hardening roadmap, or validation of core tenant controls before deeper governance, Copilot, or insurance work.

WHAT YOU RECEIVE

Leadership output

- Executive security scorecard summarizing overall posture, key risk themes, and remediation priorities.

Technical review

- Identity and access: MFA, Conditional Access, authentication settings, available user-risk indicators, guest access, and administrative-role exposure.
- Privileged access: highly privileged roles, Global Administrator sprawl, assignment hygiene, and least-privilege recommendations.
- Exchange Online: anti-phishing, anti-malware, Safe Links, Safe Attachments, forwarding, transport, and mailbox security signals where available.
- SharePoint, OneDrive, and Teams: tenant sharing posture, external-sharing settings, collaboration controls, and common exposure indicators.
- Device and endpoint readiness considerations, with validation guidance for compliance, join state, Microsoft Defender posture, and endpoint-management evidence where that data is not collected.

Remediation

- Risk-ranked findings with severity, business impact, technical context, and recommended action.
- Prioritized roadmap sequenced for practical implementation rather than an unfiltered control list.

Evidence boundary Findings reflect the tenant telemetry, licensed features, Microsoft exports, and customer-provided evidence available during the engagement. Items that cannot be directly validated are clearly identified for manual review or attestation.

Microsoft 365 Security & Data Governance

OVERVIEW

Evaluate security and governance controls across identity, collaboration, sharing, data protection, information lifecycle, and compliance readiness.

BEST FIT

Designed for clients that need a deeper control assessment covering collaboration exposure, sensitive-data protection, retention, and governance operating-model maturity.

WHAT YOU RECEIVE**Reports**

- Executive Summary for leadership covering posture, major risks, business impact, and remediation themes.
- Detailed Findings report for technical teams covering identity, access, collaboration, sharing, data protection, retention, and administrative governance.

Technical and governance review

- Identity and privileged access: MFA, Conditional Access, guest access, administrative-role exposure, and high-risk governance concerns.
- SharePoint, OneDrive, and Teams: external sharing, broad-access patterns, ownership concerns, and collaboration-control recommendations.
- Sensitivity labels, DLP, retention, and information-protection readiness where Microsoft Purview evidence is available or imported.
- Data lifecycle and ownership: stale, ownerless, externally shared, or poorly governed collaboration areas where evidence is available.

Remediation and evidence

- Risk-ranked roadmap connecting technical findings to business impact and governance outcomes.
- Scope boundary identifying what was technically observed, imported, or dependent on supplemental evidence or customer attestation.

Evidence boundary Findings reflect the tenant telemetry, licensed features, Microsoft exports, and customer-provided evidence available during the engagement. Items that cannot be directly validated are clearly identified for manual review or attestation.

Microsoft 365 Copilot & AI Readiness

OVERVIEW

Determine whether Microsoft 365 data access, permissions, licensing, and governance controls are ready for Copilot and broader AI adoption.

BEST FIT

Useful when preparing for Microsoft 365 Copilot, expanding early adoption, or establishing governance before enabling AI-assisted search, summarization, agents, connectors, or automation.

WHAT YOU RECEIVE

Leadership output

- Executive readiness scorecard with readiness domains, risk ratings, priorities, and a roadmap for safer rollout.

Readiness review

- Technical and licensing baseline using observed Microsoft 365 and Copilot licensing evidence where available.
- App-consent posture and the risk of unmanaged AI applications or connectors accessing organizational data.
- Conditional Access coverage for workload identities and possible AI-agent identities.
- SharePoint and OneDrive exposure, using available tenant sharing data, Data Access Governance exports, site inventory, crown-jewel scope, and targeted unique-permission checks.
- Oversharing evidence covering anonymous links, organization-wide links, Everyone except external users, crown-jewel anomalies, and Restricted Content Discovery/Restricted Access Control tracking.
- Sensitivity-label taxonomy, policy readiness, and encryption considerations for sensitive content.
- Summary of workload identities with high- or medium-confidence indicators of AI-agent behavior, without exposing the full identity inventory.

Manual validation

- Checklist for controls requiring customer evidence or Microsoft portal exports, including endpoint update channel, network egress, Power Platform controls, PAYG metering, and agent-publishing governance.

Evidence boundary Findings reflect the tenant telemetry, licensed features, Microsoft exports, and customer-provided evidence available during the engagement. Items that cannot be directly validated are clearly identified for manual review or attestation.

Microsoft 365 Copilot & AI Agent / Non-Human Identity

OVERVIEW

Identify AI-related applications, agent identities, service principals, and other non-human identities across Microsoft 365, Entra ID, and Azure.

BEST FIT

Security, identity, and technology leaders concerned about shadow AI, AI agents, app registrations, automation identities, unmanaged connectors, app-only permissions, credential risk, or ownership gaps.

WHAT YOU RECEIVE

Reports

- Executive Summary for leadership covering risk posture, top risks, business impact, and remediation themes.
- Technical Findings report with detailed records for service principals, applications, Copilot signals, AI-agent confidence, permissions, credentials, ownership, and available Azure AI observations.

Identity review

- Inventory of service principals with application permissions, including high-privilege Microsoft Graph access.
- App registrations and enterprise applications with expired, non-expiring, or soon-to-expire secrets and certificates.
- Recently created or modified service principals and app registrations within the agreed lookback window.
- Keyword-based identification of AI, agent, bot, assistant, Copilot, connector, and automation applications.
- Ownership review for service principals and app registrations, including identities without an assigned owner.
- Confidence classification that distinguishes High Confidence, Medium Confidence, Unverified - Keyword Only, and non-established AI-agent signals.

Supporting context

- Available SharePoint/OneDrive exposure, Copilot license and usage, and Azure AI resource or spend observations are incorporated when the relevant evidence is collected or imported.

Evidence boundary Findings reflect the tenant telemetry, licensed features, Microsoft exports, and customer-provided evidence available during the engagement. Items that cannot be directly validated are clearly identified for manual review or attestation.

Cyber Insurance Evidence Pack

OVERVIEW

Create a point-in-time evidence package that supports cyber insurance applications and renewals with documented Microsoft 365 security observations.

BEST FIT

Built for teams preparing for renewal, underwriting follow-up, or client evidence requests involving Microsoft 365, Entra ID, Defender, Copilot, AI agents, non-human identity, or Azure AI.

WHAT YOU RECEIVE**Leadership and underwriting output**

- Executive evidence summary with priority exceptions, evidence checklist, and control-area status.
- Definitions and insurance-mapping section connecting report terminology with common underwriting concerns.
- Control-map summary grouped by themes such as Identity/MFA, Data Security/Backups, Privileged Access Management, Endpoint Detection & Response, and security governance.

Mapped evidence

- SharePoint and OneDrive exposure evidence where collected or imported, mapped to relevant underwriting concerns.
- Evidence-classification labels distinguishing observed telemetry, Microsoft exports, supplemental evidence, manual review, and customer attestation.
- Detailed evidence table explaining each object, privileged permission or credential evidence, observed condition, classification, and any additional evidence required.

Exceptions and boundaries

- Items that should be remediated, validated, or disclosed before relying on simple yes/no questionnaire answers.
- Clear scope statement explaining what was observed and what may require portal exports, policy documents, screenshots, or customer attestation.

Evidence boundary Findings reflect the tenant telemetry, licensed features, Microsoft exports, and customer-provided evidence available during the engagement. Items that cannot be directly validated are clearly identified for manual review or attestation.